ルールを使用した侵入ポリシーの調整

侵入ポリシーの [ルール] ページを使用して、共有オブジェクトのルール、標準テキスト ルール、およびプリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。オプションで、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。詳細については、インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーの Web インターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーに関する制約事項（23-13 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入防御ルール タイプについて（32-2 ページ）では、侵入ポリシーで表示または設定可能な侵入ルールとプリプロセッサ ルールについて説明します。
- 侵入ポリシー内のルールの表示（32-3 ページ）では、[ルール（Rules）] ページでルールの順序を変更したり、ページ上のアイコンを解釈したり、ルール詳細に焦点を当てたりするための方法について説明します。
- 侵入ポリシー内のルールのフィルタリング（32-11 ページ）では、ルール フィルタを使用して、ルール設定を適用するルールを見つける方法について説明します。
- ルール状態の設定（32-23 ページ）では、[ルール（Rules）] ページでルールを有効または無効にする方法について説明します。
- ポリシー単位の侵入イベント通知のフィルタリング（32-26 ページ）では、特定のルールに対するイベント フィルタリングしきい値の設定方法と特定のルールの抑制方法について説明します。
- 動的ルール状態の追加（32-34 ページ）では、一致するトラフィックでレート異常が検出されたときに動的にトリガーとして使用されるルール状態の設定方法について説明します。
- SNMP アラートの追加（32-38 ページ）では、SNMP アラートを特定のルールに関連付ける方法について説明します。
- ルール コメントの追加（32-39 ページ）では、侵入ポリシー内のルールにコメントを追加する方法について説明します。

侵入防御ルール タイプについて

ライセンス：Protection

侵入ポリシーには、侵入ルールとプリプロセッサ ルールという 2 つのルール タイプが含まれています。

侵入ルールは、ネットワーク上の脆弱性を悪用する試みを検出するキーワードと引数の指定されたセットで、ネットワーク トラフィックを分析してルール内の基準が満たされているかどうかをチェックします。システムは各ルールで指定された条件をパケットに照らし合わせます。ルールで指定されたすべての条件にパケット データが一致する場合、ルールがトリガーされます。システムには、シスコ脆弱性調査チーム（VRT）が作成した次の 2 種類の侵入ルールが付属しています。共有オブジェクトのルールは、コンパイルされ、変更できません（送信元ポート、宛先ポート、IP アドレスなどのルール ヘッダー情報を除く）。標準テキスト ルールは、ルールの新しいカスタム インスタンスとして保存して変更できます。

システムには、プリプロセッサに関連付けられたルールであるプリプロセッサ ルールとパケット デコーダ検出オプションも付属しています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサ ルールがデフォルトで無効になっているため、システムにプリプロセッサ ルールに対するイベントの生成とインライン展開での違反パケットの破棄を指示する場合は、これらのルールを有効にする（つまり、[イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定する）必要があります。

VRT が、システムに付属のデフォルト侵入ポリシー用のシスコの共有オブジェクトのルール、標準テキスト ルール、およびプリプロセッサ ルールのデフォルト ルール状態を決定します。

次の表に、FireSIGHT システムに付属しているルール タイプの説明を示します。

表 32-1　ルール タイプ

タイプ（Type）	説明
共有オブジェクトのルール	C ソース コードからコンパイルされたバイナリ モジュールとして配布されるシスコ脆弱性調査チーム（VRT）によって作成された侵入ルール。共有オブジェクトのルールを使用して、標準テキスト ルールでは不可能な方法で攻撃を検出できます。共有オブジェクトのルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム共有オブジェクトのルールとしてのルールの新しいインスタンスの保存のみです。共有オブジェクトのルールには、GID（ジェネレータ ID）の 3 が割り当てられます。詳細については、既存のルールの変更（36-114 ページ）を参照してください。
標準テキスト ルール	VRT によって作成された侵入ルール、コピーされて新しいカスタム ルールとして保存された侵入ルール、ルール エディタを使用して作成された侵入ルール、またはユーザがローカル マシン上で作成してインポートしたローカル ルールとしてインポートされた侵入ルール。VRT によって作成された標準ルール内のルール キーワードと引数は変更できません。実行できるのは、ルール内で使用されている変数の変更か、送信元ポート、宛先ポート、IP アドレスなどの要素の変更とカスタム標準テキスト ルールとしてのルールの新しいインスタンスの保存のみです。詳細については、既存のルールの変更（36-114 ページ）、侵入ルールの理解と作成（36-1 ページ）、およびローカル ルール ファイルのインポート（66-22 ページ）を参照してください。VRT によって作成された標準テキスト ルールには、GID（ジェネレータ ID）の 1 が割り当てられます。ルール エディタを使用して作成した、または、ローカル ルールとしてインポートしたカスタム標準テキスト ルールには 1000000 以上の SID（シグニチャ ID）が割り当てられます。
プリプロセッサ ルール	パケット デコーダの検出オプションまたは FireSIGHT システムに付属のプリプロセッサの 1 つに関連付けられたルール。プリプロセッサ ルールによってイベントを生成するには、プリプロセッサ ルールを有効にする必要があります。このルールには、デコーダ固有またはプリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。詳細については、ジェネレータ ID の表を参照してください。

侵入ポリシー内のルールの表示

ライセンス：Protection

侵入ポリシーでのルールの表示方法を調整でき、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

[ルール（Rules）] ページには次の 4 つの主な機能領域があります。

- フィルタリング機能：詳細については、侵入ポリシー内のルールのフィルタリング（32-11 ページ）を参照してください。
- ルール属性メニュー：詳細については、ルール状態の設定（32-23 ページ）、ポリシー単位の侵入イベント通知のフィルタリング（32-26 ページ）、動的ルール状態の追加（32-34 ページ）、SNMP アラートの追加（32-38 ページ）、およびルール コメントの追加（32-39 ページ）を参照してください。
- ルール一覧：詳細については、[ルール（Rules）] ページのカラムの表を参照してください。
- ルールの詳細：詳細については、ルール詳細の表示（32-5 ページ）を参照してください。

さまざまな基準に基づいてルールをソートすることもできます。詳細については、ルール画面のソート（32-5 ページ）を参照してください。

カラム見出しとして使用されているアイコンは、設定項目にアクセスするためのメニュー バー内のメニューに対応していることに注意してください。たとえば、[ルール状態（Rule State）] メニューは、[ルール状態（Rule State）] カラムと同じアイコン（）でマークされています。

次の表に、[ルール（Rules）] ページのカラムの説明を示します。

表 32-2　[ルール（Rules）] ページのカラム

見出し	説明	詳細
GID	ルールのジェネレータ ID（GID）を表す整数。	プリプロセッサ ジェネレータ ID の読み取り（41-44 ページ）
SID	ルールの一意の識別子として機能する Snort ID（SID）を表す整数。	プリプロセッサ ジェネレータ ID の読み取り（41-44 ページ）
メッセージ	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。	イベント メッセージの定義（36-13 ページ）
	ルールのルール状態。次の 3 つのうちのいずれかの状態になります。 • ドロップしてイベントを生成する（） • イベントを生成する（） • 無効（） ルール状態アイコンをクリックすることによって、ルールの [ルール状態の設定（Set rule state）] ダイアログボックスにアクセスできることに注意してください。	ルール状態の設定（32-23 ページ）
	ルールの FireSIGHT 推奨ルール状態。	ネットワーク資産に応じた侵入防御の調整（33-1 ページ）

表 32-2　[ルール(Rules)] ページのカラム(続き)

見出し	説明	詳細
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。	ポリシー単位の侵入イベント通知のフィルタリング(32-26 ページ)
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。	動的ルール状態の追加(32-34 ページ)
	ルールに対して設定されたアラート(現在は SNMP アラートのみ)。	SNMP アラートの追加(32-38 ページ)
	ルールに追加されたコメント。	ルール コメントの追加(32-39 ページ)

レイヤのドロップダウンリストを使用して、ポリシー内の他のレイヤの [ルール(Rules)] ページに切り替えることもできます。ポリシーにレイヤを追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [ルール(Rules)] ページと、元は `My Changes` という名前だったポリシー階層の [ルール(Rules)] ページだけであることに注意してください。これらのビューの一方を変更すると、もう一方も同じように変更されることにも注意してください。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用(24-1 ページ)を参照してください。ドロップダウンリストには、読み取り専用の基本ポリシーの [ルール(Rules)] ページも表示されます。基本ポリシーの詳細については、基本レイヤについて(24-3 ページ)を参照してください。

侵入ポリシー内のルールを表示する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [侵入(Intrusion)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

手順 3　[ポリシー情報(Policy Information)] ページで [ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ナビゲーション パネルの境界線の上にある [ルール(Rules)] を選択すると、同じルール一覧が表示されることに注意してください。このビューでポリシー内のすべてのルール属性を表示して設定できます。

ルール画面のソート

ライセンス：Protection

[ルール（Rules）] ページでは、見出しタイトルまたはアイコンをクリックすることによって、ルールをいずれかのカラムでソートできます。

見出しまたはアイコン上の上矢印（▲）または下矢印（▶）は、そのカラムを基準として、その方向にソートが実行されることを意味していることに注意してください。

侵入ポリシー内でルールをソートする方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　ソートの基準とするカラムの一番上のタイトルまたはアイコンをクリックします。

ルールがそのカラムのカラム見出しに表示された矢印が示す方向でソートされます。反対方向でソートするには、見出しを再度クリックします。ソート順と矢印が反転します。

ルール詳細の表示

ライセンス：Protection

[ルールの詳細（Rule Detail）] ビューで、ルール ドキュメント、FireSIGHT 推奨、およびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことに注意してください。

表 32-3　ルールの詳細

項目	説明	詳細
要約	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこの行が表示されます。	イベント情報の表示（41-27 ページ）
ルール状態（Rule State）	ルールの現在のルール状態。ルール状態が設定された階層も示します。	ルール状態の設定（32-23 ページ）、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）

表 32-3　ルールの詳細（続き）

項目	説明	詳細
FireSIGHT 推奨（Recommendation）	FireSIGHT 推奨が生成されている場合のルールの推奨ルール状態。	ネットワーク資産に応じた侵入防御の調整（33-1 ページ）
ルールのオーバーヘッド（Rule Overhead）	システム パフォーマンスに対するルールの潜在的影響とルールが誤検出を引き起こす確率。	ルール オーバーヘッドについて（33-3 ページ）
しきい値	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。	ルールのしきい値の設定（32-7 ページ）
抑制（Suppressions）	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。	ルールの抑制の設定（32-8 ページ）
動的状態（Dynamic State）	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。	ルールの動的ルール状態の設定（32-8 ページ）
アラート（Alerts）	このルールに現在設定されているアラートと、ルールのアラートを追加するための機能。現在は、SNMP アラートのみがサポートされています。	ルールの SNMP アラートの設定（32-10 ページ）
説明	このルールに追加されたコメントと、ルールのコメントを追加するための機能。	ルールに関するルール コメントの追加（32-10 ページ）
資料	シスコ脆弱性調査チーム（VRT）から提供される現在のルールのルール ドキュメント。	パケット ビュー アクションの使用（41-31 ページ）

ルール詳細を表示する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　ルール詳細を表示するルールを強調表示します。

手順 5　[詳細の表示（Show details）] をクリックします。

[ルールの詳細（Rule Detail）] ビューが表示されます。詳細を再度非表示にするには、[詳細の非表示（Hide details）] をクリックします。

ヒント　[ルール（Rules）] ビューでルールをダブルクリックすることによって、[ルールの詳細（Rule Detail）] を開くこともできます。

ルールのしきい値の設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。しきい値設定の詳細については、イベントしきい値の設定（32-26 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細でしきい値を設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　[しきい値（Thresholds）] の横にある [追加（Add）] をクリックします。

[しきい値の設定（Set Threshold）] ダイアログボックスが表示されます。

手順 2　[タイプ（Type）] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限（Limit）] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値（Threshold）] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

手順 3　[追跡対象（Track By）] ドロップダウンリストから、[送信元（Source）] または [宛先（Destination）] を選択し、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを指定します。

手順 4　[カウント（Count）] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

手順 5　[秒（Seconds）] フィールドで、イベント インスタンスを追跡する期間（秒数）を指定する 0 から 2147483647 までの数を入力します。

手順 6　[OK] をクリックします。

システムが、しきい値を追加し、[イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

ルールの抑制の設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの 1 つまたは複数の抑制を設定できます。抑制の詳細については、侵入ポリシー単位の抑制の設定（32-31 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で抑制を設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　[抑制（Suppressions）] の横にある [追加（Add）] をクリックします。

[抑制の追加（Add Suppression）] ダイアログボックスが表示されます。

手順 2　[抑制タイプ（Suppression Type）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール（Rule）] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元（Source）] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先（Destination）] を選択します。

手順 3　抑制タイプに [送信元（Source）] または [宛先（Destination）] を選択した場合は、[ネットワーク（Network）] フィールドが表示されます。[ネットワーク（Network）] フィールドで、IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを入力します。侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 4　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ルールの動的ルール状態の設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの 1 つまたは複数の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されることに注意してください。動的ルール状態の詳細については、動的ルール状態について（32-34 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で動的ルール状態を設定する方法:

アクセス: Admin/Intrusion Admin

手順 1　[動的状態(Dynamic State)] の横にある [追加(Add)] をクリックします。

[レート ベースのルール状態の追加(Add Rate-Based Rule State)] ダイアログボックスが表示されます。

手順 2　[追跡対象(Track By)] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元(Source)] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先(Destination)] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール(Rule)] を選択します。

手順 3　オプションで、[追跡対象(Track By)] を [送信元(Source)] または [宛先(Destination)] に設定した場合は、[ネットワーク(Network)] フィールドに追跡する各ホストの IP アドレスを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィックス長表記を使用する方法については、IP アドレスの表記規則(1-24 ページ)を参照してください。

手順 4　[レート(Rate)] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント(Count)] フィールドで、0 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [秒(Seconds)] フィールドで、0 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

手順 5　[新しい状態(New State)] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを選択します。

- イベントを生成する場合は、[イベントを生成する(Generate Events)] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットを破棄する場合、または、パッシブ展開でイベントを生成する場合は、[ドロップしてイベントを生成する(Drop and Generate Events)] を選択します。
- アクションを実行しない場合は、[無効(Disabled)] を選択します。

手順 6　[タイムアウト(Timeout)] フィールドに、1 ～ 2147483647(約 68 年)の整数を使用して、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を指定します。

手順 7　[OK] をクリックします。

システムが、動的ルール状態を追加し、[動的状態(Dynamic State)] カラムのルールの横に動的状態アイコン( )を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ルールの SNMP アラートの設定

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールの SNMP アラートを設定できます。SNMP アラートの詳細については、SNMP アラートの追加（32-38 ページ）を参照してください。

ルール詳細で SNMP アラートを追加する方法：

アクセス：Admin/Intrusion Admin

手順 1　[アラート（Alerts）] の横にある [SNMP アラートの追加（Add SNMP Alert）] をクリックします。

システムが、アラートを追加し、[アラート（Alerting）] カラムのルールの横にアラート アイコン（ ）を表示します。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

ルールに関するルール コメントの追加

ライセンス：Protection

[ルールの詳細（Rule Detail）] ページで、ルールに関するルール コメントを追加できます。ルール コメントの詳細については、ルール コメントの追加（32-39 ページ）を参照してください。

ルール詳細でコメントを追加する方法：

アクセス：Admin/Intrusion Admin

手順 1　[コメント（Comments）] の横にある [追加（Add）] をクリックします。

[コメントの追加（Add Comment）] ダイアログボックスが表示されます。

手順 2　[コメント（Comments）] フィールドに、ルール コメントを入力します。

手順 3　[OK] をクリックします。

システムが、コメントを追加し、[コメント（Comments）] カラムのルールの横にコメント アイコン（ ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、ルール コメント セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

侵入ポリシー内のルールのフィルタリング

ライセンス：Protection

[ルール（Rules）] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

作成したフィルタが [フィルタ（Filter）] テキストボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

[カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、[プリプロセッサ（Preprocessor）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,os-linux"`」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコン（  ）をクリックします。

詳細は、次のトピックを参照してください。

- 侵入ポリシー内のルール フィルタリングについて（32-11 ページ）
- 侵入ポリシー内のルール フィルタの設定（32-22 ページ）

侵入ポリシー内のルール フィルタリングについて

ライセンス：Protection

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[ルール（Rules）] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

詳細については、次の項を参照してください。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン（32-12 ページ）
- ルール構成フィルタについて（32-15 ページ）
- ルール コンテンツ フィルタについて（32-18 ページ）
- ルール カテゴリについて（32-20 ページ）
- ルール フィルタの直接編集（32-20 ページ）

侵入ポリシー ルール フィルタを作成するためのガイドライン

ライセンス: Protection

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [ルール(Rules)] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには、展開して個別のルールにドリルダウンするための複数のレベルが設定されています。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の経験則をフィルタの作成に役立ててください。

- キーワード([ルール設定(Rule Configuration)]、[ルール コンテンツ(Rule Content)]、[プラットフォーム特有(Platform Specific)]、および [優先度(Priority)]) 以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開されて使用可能なキーワードが一覧表示されます。

  基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

  そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

  たとえば、フィルタ パネルの [ルール設定(Rule Configuration)] > [推奨(Recommendation)] で [ドロップしてイベントを生成する(Drop and Generate Events)] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキストボックスに追加されます。その後で、[ルール設定(Rule Configuration)] > [推奨(Recommendation)] で [イベントを生成する(Generate Events)] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

- キーワード([カテゴリ(Category)]、[分類(Classifications)]、[Microsoft 脆弱性(Microsoft Vulnerabilities)]、[Microsoft ワーム(Microsoft Worms)]、[優先度(Priority)]、および [ルール アップデート(Rule Update)]) になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

  このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

  たとえば、フィルタ パネルの [カテゴリ(Category)] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[カテゴリ(Category)] で [os-windows] をクリックすると、フィルタが「`Category:"os-windows"`」に変更されます。

- [ルール コンテンツ(Rule Content)] の下の [参照(Reference)] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。参照キーワードのいずれかを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、キーワードが既存のフィルタに追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

  たとえば、フィルタ パネルで [ルール コンテンツ(Rule Content)] > [参照(Reference)] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう求められます。「`2007`」と入力すると、「`CVE:"2007"`」がフィルタ テキストボックスに追加されます。別の例では、フィルタ パネルで [ルール コンテンツ(Rule Content)] > [参照(Reference)] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう求められます。「`2007`」と入力すると、「`Reference:"2007"`」がフィルタ テキストボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

  たとえば、フィルタ パネルの [カテゴリ（Category）] で [os-linux] をクリックすると、「`Category:"os-linux"`」がフィルタ テキストボックスに追加されます。その後で、[Microsoft 脆弱性（Microsoft Vulnerabilities）] で [MS00-006] をクリックすると、フィルタが「`Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`」に変更されます。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[カテゴリ（Category）] で [プリプロセッサ（preprocessor）] を選択してから、[ルール コンテンツ（Rule Content）] > [GID] の順に選択して、「`116`」と入力すると、プリプロセッサ ルールで、**かつ**、GID が 116 のすべてのルールを取得する「`Category: "preprocessor" GID:"116"`」というフィルタが返されます。

- [カテゴリ（Category）]、[Microsoft 脆弱性（Microsoft Vulnerabilities）]、[Microsoft ワーム（Microsoft Worms）]、[プラットフォーム特有（Platform Specific）]、および [優先度（Priority）] の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[カテゴリ（Category）] から [os-linux] と [os-windows] を選択すれば、`os-linux` カテゴリまたは `os-windows` カテゴリ内のルールを取得する「`Category:"os-windows,app-detect"`」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールが **dos** カテゴリでフィルタ処理された場合と **High** 優先度でフィルタ処理された場合はともに、DOS Cisco attempt rule（SID 1545）が表示されます。

（注） シスコ VRT がルール更新メカニズムを使用してルール フィルタを追加または削除する場合があります。

[ルール（Rules）] ページ上のルールは、共有オブジェクトのルール（ジェネレータ ID 3）と標準テキスト ルール（ジェネレータ ID 1）のどちらかであることに注意してください。次の表に、さまざまなルール フィルタの説明を示します。

表 32-4　ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
ルール設定（Rule Configuration）	ルールの設定に基づいてルールを検索します。ルール構成フィルタについて（32-15 ページ）を参照してください。	なし	グループ	キーワード
ルール コンテンツ（Rule Content）	ルールの内容に基づいてルールを検索します。ルール コンテンツ フィルタについて（32-18 ページ）を参照してください。	なし	グループ	キーワード
カテゴリ（Category）	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。ルール カテゴリについて（32-20 ページ）を参照してください。	○	キーワード	引数

表 32-4　ルール フィルタ グループ(続き)

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
分類(Classifications)	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。侵入イベントの検索(41-46 ページ)および侵入イベント分類の定義(36-13 ページ)を参照してください。	なし	キーワード	引数
Microsoft 脆弱性(Microsoft Vulnerabilities)	Microsoft セキュリティ情報番号に従ってルールを検索します。	○	キーワード	引数
Microsoft ワーム(Microsoft Worms)	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	○	キーワード	引数
プラットフォーム特有(Platform Specific)	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
プリプロセッサ(Preprocessors)	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成するためには、そのオプションに関連付けられたプリプロセッサ ルールを有効にする必要があることに注意してください。ルール状態の設定(32-23 ページ)を参照してください。	○	グループ	サブグループ
[プライオリティ(Priority)]	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール(つまり、ユーザが作成したルール)は優先度グループに表示されないことに注意してください。	○	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
ルール アップデート(Rule Update)	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	なし	キーワード	引数

ルール構成フィルタについて

ライセンス：Protection

[ルール（Rules）] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。たとえば、ルール状態が推奨ルール状態と一致しない一連のルールを表示する場合は、[推奨と一致しない（Does not match recommendation）] を選択することによってルール状態をフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [ドロップしてイベントを生成する（Drop and Generate Events）] をクリックすると、「`Recommendation:"Drop and Generate Events"`」がフィルタ テキストボックスに追加されます。その後で、[ルール設定（Rule Configuration）] > [推奨（Recommendation）] で [イベントを生成する（Generate Events）] をクリックすると、フィルタが「`Recommendation:"Generate Events"`」に変更されます。

フィルタ処理に使用可能なルール構成設定に関する詳細については、次の手順を参照してください。

ルール状態フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ルール設定（Rule Configuration）] で、[ルール状態（Rule State）] をクリックします。

手順 2　[ルール状態（Rule State）] ドロップダウンリストから、フィルタ条件のルール状態を選択します。

- イベントを生成するだけのルールを検索するには、[イベントを生成する（Generate Events）] を選択して、[OK] をクリックします。
- イベントを生成して一致するパケットをドロップするよう設定されたルールを検索するには、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択して、[OK] をクリックします。
- 無効になっているルールを検索するには、[無効（Disabled）] を選択して、[OK] をクリックします。
- ルール状態が推奨状態と一致しないルールを検索するには、[推奨と一致しない（Does not match recommendation）] を選択して、[OK] をクリックします。

最新のルール状態に基づいてルールを表示するように [ルール（Rules）] ページが更新されます。

推奨フィルタを使用する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ルール設定（Rule Configuration）] で、[推奨（Recommendation）] をクリックします。

手順 2　[推奨（Recommendation）] ドロップダウン リストから、フィルタ条件となる FireSIGHT ルール状態の推奨事項を選択し、[OK] をクリックします。

推奨ルール状態に基づいてルールを表示するように [ルール（Rules）] ページが更新されます。

しきい値フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ルール設定(Rule Configuration)] で、[しきい値(Threshold)] をクリックします。

手順 2　[しきい値(Threshold)] ドロップダウンリストから、フィルタ条件のしきい値設定を選択します。

- しきい値タイプが `limit` のルールを検索するには、[制限(Limit)] を選択して、[OK] をクリックします。
- しきい値タイプが `threshold` のルールを検索するには、[しきい値(Threshold)] を選択して、[OK] をクリックします。
- しきい値タイプが `both` のルールを検索するには、[両方(Both)] を選択して、[OK] をクリックします。
- しきい値が `source` によって追跡されるルールを検索するには、[送信元(Source)] を選択して、[OK] をクリックします。
- しきい値が `Destination` によって追跡されるルールを検索するには、[宛先(Destination)] を選択して、[OK] をクリックします。
- しきい値が設定された任意のルールを検索するには、[すべて(All)] を選択して、[OK] をクリックします。

フィルタで指定されたしきい値のタイプがルールに適用されているルールを表示するように [ルール(Rules)] ページが更新されます。

抑制フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ルール設定(Rule Configuration)] で、[抑制(Suppression)] をクリックします。

手順 2　[抑制(Suppression)] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- イベントがそのルールによって検査されるパケットに抑制されたルールを検索するには、[ルール別(By Rule)] を選択して、[OK] をクリックします。
- イベントがトラフィックの送信元に基づいて抑制されるルールを検索するには、[送信元別(By Source)] を選択して、[OK] をクリックします。
- イベントがトラフィックの宛先に基づいて抑制されるルールを検索するには、[宛先別(By Destination)] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[すべて(All)] を選択して、[OK] をクリックします。

フィルタで指定された抑制のタイプがルールに適用されているルールを表示するように [ルール(Rules)] ページが更新されます。

動的状態フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ルール設定（Rule Configuration）] で、[動的状態（Dynamic State）] をクリックします。

手順 2　[動的状態（Dynamic State）] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- 動的状態がそのルールによって検査されるパケットに設定されたルールを検索するには、[ルール別（By Rule）] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの送信元に基づくパケットに設定されたルールを検索するには、[送信元別（By Source）] を選択して、[OK] をクリックします。
- 動的状態がトラフィックの宛先に基づいて設定されたルールを検索するには、[宛先別（By Destination）] を選択して、[OK] をクリックします。
- `Generate Events` の動的状態が設定されたルールを検索するには、[イベントを生成する（Generate Events）] を選択して、[OK] をクリックします。
- `Drop and Generate Events` の動的状態が設定されたルールを検索するには、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択して、[OK] をクリックします。
- `Disabled` の動的状態が設定されたルールを検索するには、[無効（Disabled）] を選択して、[OK] をクリックします。
- 抑制が設定された任意のルールを検索するには、[すべて（All）] を選択して、[OK] をクリックします。

フィルタで指定された動的ルール状態がルールに適用されているルールを表示するように [ルール（Rules）] ページが更新されます。

アラート フィルタの使用方法:

アクセス: Admin/Intrusion Admin

手順 1　[ルール設定（Rule Configuration）] で、[アラート（Alert）] をクリックします。

手順 2　[アラート（Alert）] ドロップダウンリストから、**SNMP** 別にフィルタ処理するアラート設定を選択します。

手順 3　[OK] をクリックします。

[ルール（Rules）] ページが更新され、アラート フィルタを適用したルールが表示されます。

コメント フィルタを使用する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ルール設定（Rule Configuration）] で、[コメント（Comment）] をクリックします。

手順 2　[コメント（Comment）] フィールドに、フィルタ条件のコメント テキスト文字列を入力し、[OK] をクリックします。

ルールに適用されるコメントにフィルタで指定された文字列が含まれているルールを表示するように [ルール（Rules）] ページが更新されます。

ルール コンテンツ フィルタについて

ライセンス：Protection

[ルール（Rules）] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ条件とする引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [ルール コンテンツ（Rule Content）] で [SID] をクリックすると、ポップアップ ウィンドウが開いて SID の入力が促されます。「1045」と入力すると、「SID:"1045"」がフィルタ テキストボックスに追加されます。その後で、再度 [SID] をクリックして、SID フィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変更されます。

フィルタ処理に使用可能なルール コンテンツの詳細については、次の表を参照してください。

表 32-5　ルール コンテンツ フィルタ

このフィルタを使用する場合のクリック対象	次の操作	結果
メッセージ	フィルタ条件のメッセージ文字列を入力して、[OK] をクリックします。	メッセージ フィールドで指定された文字列を含むルールを検索します。
SID	フィルタ条件の SID 番号を入力して、[OK] をクリックします。	指定された SID が割り当てられたルールを検索します。
GID	フィルタ条件の GID 番号を入力して、[OK] をクリックします。	指定された GID が割り当てられたルールを検索します。
参照	フィルタ条件の参照文字列を入力して、[OK] をクリックします。 フィルタ条件とする特定のタイプの参照に対する文字列を入力するには、[CVE ID]、[URL]、[Bugtraq ID]、[Nessus ID]、[Arachnids ID]、または [Mcafee ID] を選択し、文字列を入力して [OK] をクリックします。	参照フィールドで指定された文字列を含むルールを検索します。
アクション（Action）	フィルタ処理するアクションを選択します。 • アラート ルールを検索するには、[アラート（Alert）] を選択して、[OK] をクリックします。 • パス ルールを検索するには、[パス（Pass）] を選択して、[OK] をクリックします。	alert または pass で始まるルールを検索します。
プロトコル	フィルタ条件のプロトコル（[ICMP]、[IP]、[TCP]、または [UDP]）を選択し、[OK] をクリックします。	選択されたプロトコルを含むルールを検索します。

表 32-5　ルール コンテンツ フィルタ（続き）

このフィルタを使用する場合のクリック対象	次の操作	結果
方向（Direction）	フィルタ処理する方向設定を選択します。 • 特定の方向に移動するトラフィックを検査するルールを検索するには、[指向性（Directional）] を選択して、[OK] をクリックします。 • 送信元と宛先の間をどちらの方向にも移動するトラフィックを検査するルールを検索するには、[双方向（Bidirectional）] を選択して、[OK] をクリックしてします。	ルールに、指定された方向設定が含まれているかどうかに基づいてルールを検索します。
ソース IP	フィルタ条件の送信元 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
宛先 IP（Destination IP）	フィルタ条件の宛先 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィックス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
ソース ポート	フィルタ条件の送信元ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された送信元ポートを含むルールを検索します。
接続先ポート（Destination port）	フィルタ条件の宛先ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された宛先ポートを含むルールを検索します。

表 32-5　ルール コンテンツ フィルタ（続き）

このフィルタを使用する場合のクリック対象	次の操作	結果
ルールのオーバーヘッド（Rule Overhead）	フィルタ条件のルール オーバーヘッドの量（[低（Low）]、[中（Medium）]、[高（High）]、または [非常に高い（Very High）]）を選択し、[OK] をクリックします。	選択されたルール オーバーヘッドを伴うルールを検索します。
メタデータ（Metadata）	フィルタ条件のメタデータのキーと値のペアをスペースで区切って入力し、[OK] をクリックします。 たとえば、HTTP アプリケーション プロトコルに関連するメタデータを使用したルールを検索するには、「`metadata:"service http"`」と入力します。	一致するキーと値のペアを含むメタデータを使用したルールを検索します。

ルール カテゴリについて

ライセンス：Protection

FireSIGHT システムは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[ルール（Rules）] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

カテゴリ名の上にポインタを移動すると、そのカテゴリ内のルールの数を表示できます。

（注） シスコ VRT がルール更新メカニズムを使用してルール カテゴリを追加または削除する場合があります。

ルール フィルタの直接編集

ライセンス：Protection

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[ルール（Rules）] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[ルール（Rules）] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキストボックスに表示されます。

特定の値のみをサポートするキーワードの引数のリストを表示するには、ルール構成フィルタについて（32-15 ページ）、ルール コンテンツ フィルタについて（32-18 ページ）、およびルール カテゴリについて（32-20 ページ）を参照してください。キーワードのカンマ区切りの複数の引数は [カテゴリ（Category）] と [優先度（Priority）] のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、および除外文字(!)、「大なり」記号(>)、「小なり」記号(<)などの特殊な演算子をフィルタに含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ(Category)]、[メッセージ(Message)]、および [SID] の各フィールドで指定された単語が検索されます。

すべてのキーワード、キーワード引数、および文字列では大文字と小文字が区別されません。`gid` キーワードと `sid` キーワードを除くすべての引数と文字列が部分文字列として扱われます。`gid` と `sid` の引数は、完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

Keyword:*"argument"*

ここで、*Keyword* はルール タイプの表に示すフィルタ グループ内のキーワードのいずれかで、*argument* は二重引用符で囲まれ、キーワードに関連した特定のフィールド内で検索される単一の大文字と小文字が区別されない英数字文字列です。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

`gid` と `sid` を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 `123` によって `"12345"`、`"41235"`、`"45123"` などが返されます。`gid` と `sid` の引数は完全一致のみを返します。たとえば、`sid:3080` は `SID 3080` のみを返します。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [メッセージ(Message)] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 `123` は、ルール メッセージ内の文字列 `"Lotus123"` や `"123mania"` などを返し、`SID 6123` や `SID 12375` なども返します。ルールの [メッセージ(Message)] フィールドの詳細については、イベント メッセージの定義(36-13 ページ)を参照してください。ルール SID と GID の詳細については、プリプロセッサ ジェネレータ ID の読み取り(41-44 ページ)を参照してください。部分的な SID を検索するには、1 つ以上の文字列を使ってフィルタ処理できます。

すべての文字列では大文字と小文字が区別されず、部分的な文字列として扱われます。たとえば、文字列 `ADMIN`、`admin`、または `Admin` はすべて、`"admin"`、`"CFADMIN"`、`"Administrator"` などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 `"overflow attempt"` は完全一致のみを返しますが、引用符なしの 2 つの文字列 `overflow` と `attempt` で構成されるフィルタは `"overflow attempt"`、`"overflow multipacket attempt"`、`"overflow with evasion attempt"` などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

侵入ポリシー内のルール フィルタの設定

ライセンス：Protection

[ルール（Rules）] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。その後で、いずれかのページ機能を使用できます。これには、コンテキスト メニューで使用可能な機能の選択も含まれます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されている場合もされていない場合も、リスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

侵入ポリシー内の [ルール（Rules）] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

使用可能なすべてのキーワードと引数の詳細と、フィルタ パネルでのフィルタの作成方法については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）を参照してください。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたフィルタは、ルール データベース全体を検索して、一致するすべてのルールを返します。前回のフィルタ結果がページに表示されている状態でフィルタを入力すると、そのページの内容が消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[カテゴリ（Category）]、[メッセージ（Message）]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内の特定のルールに対してフィルタ処理する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられることに注意してください。詳細については、次の各項を参照してください。

- 侵入ポリシー ルール フィルタを作成するためのガイドライン（32-12 ページ）
- ルール構成フィルタについて（32-15 ページ）
- ルール コンテンツ フィルタについて（32-18 ページ）
- ルール カテゴリについて（32-20 ページ）
- ルール フィルタの直接編集（32-20 ページ）

ページが、すべての一致するルールを表示するように更新され、フィルタと一致するルールの数がフィルタ テキストボックスの上に表示されます。

手順 5　新しい設定を適用する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　オプションで、ページに表示されているルールを通常の方法で変更します。詳細については、次の各項を参照してください。

- [ルール（Rules）] ページ上でルールを有効または無効にする方法については、ルール状態の設定（32-23 ページ）を参照してください。
- ルールにしきい値設定と抑制を追加する方法については、ポリシー単位の侵入イベント通知のフィルタリング（32-26 ページ）を参照してください。
- 一致するトラフィックでレート異常が発生したときにトリガーされる動的ルール状態を設定する方法については、動的ルール状態の追加（32-34 ページ）を参照してください。
- 特定のルールに SNMP アラートを追加する方法については、SNMP アラートの追加（32-38 ページ）を参照してください。
- ルールにルール コメントを追加する方法については、ルール コメントの追加（32-39 ページ）を参照してください。

手順 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

ルール状態の設定

ライセンス：Protection

シスコ脆弱性調査チーム（VRT）が、各デフォルト ポリシー内の侵入ルールとプリプロセッサ ルールのデフォルト状態を設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。作成された侵入ポリシー ルールは、作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

ルールを [イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、または [無効（Disable）] に個別に設定することも、状態を変更するルールを選択するためのさまざまな要素でルールをフィルタ処理することもできます。インライン展開では、インライン侵入展開で [ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態を使用して悪意のあるパケットをドロップできます。[ドロップしてイベントを生成する（Drop and Generate Events）] ルール状態のルールはイベントを生成しますが、3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含むパッシブ展開ではパケットをドロップしないことに注意してください。ルールを [イベントを生成する（Generate Events）] または [ドロップしてイベントを生成する（Drop and Generate Events）] に設定すると、ルールが有効になります。ルールを [無効（Disable）] に設定すると、ルールが無効になります。

2 つのシナリオについて考えてみます。最初のシナリオでは、特定のルールのルール状態が [イベントを生成する（Generate Events）] に設定されます。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。2 つ目のシナリオでは、同じルールのルール状態が、インライン展開で [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていると仮定します。この場合は、悪意のあるパケットがネットワークを通過すると、システムがそのパケットをドロップして、侵入イベントを生成します。パケットがターゲットに到達することはありません。

侵入ポリシーでは、ルールの状態を次のいずれかに設定できます。

- システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [イベントを生成する（Generate Events）] に設定します。
- システムで特定の侵入試行を検出してから、インライン展開で一致するトラフィックが見つかった時点で攻撃を含むパケットをドロップし、侵入イベントを生成する場合、あるいは（3D9900 または シリーズ 3 デバイスのインライン インターフェイス セットがタップ モードの場合を含む）パッシブ展開で一致するトラフィックが見つかった時点で侵入イベントを生成する場合には、ルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。

  システムでパケットをドロップする場合は、インライン展開で侵入ポリシーを廃棄ルールに設定する必要があることに注意してください。詳細については、インライン展開でのドロップ動作の設定（31-6 ページ）を参照してください。
- システムで一致するトラフィックを評価しない場合は、ルール状態を [無効（Disable）] に設定します。

廃棄ルールを使用するには、次の手順を実行する必要があります。

- 侵入ポリシーで [インライン時にドロップ（Drop when Inline）] オプションを有効にします。
- ルールと一致するすべてのパケットをドロップする必要があるすべてのルールのルール状態を [ドロップしてイベントを生成する（Drop and Generate Events）] に設定します。
- 侵入ポリシーに関連付けられたアクセス コントロール ルールを含むアクセス コントロール ポリシーを、インライン セットを使用する管理対象デバイスに適用します。

[ルール（Rules）] ページのルールのフィルタ処理は、廃棄ルールとして設定するルールを探すときに役立ちます。詳細については、侵入ポリシー内のルールのフィルタリング（32-11 ページ）を参照してください。

ルール構造、ルール キーワードとそのオプション、およびルール作成構文については、侵入ルールの理解と作成（36-1 ページ）を参照してください。

VRT がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

1 つ以上のルールのルール状態を変更する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

このページには、有効なルールの総数、[イベントを生成する（Generate Events）] に設定された有効なルールの総数、および [ドロップしてイベントを生成する（Drop and Generate Events）] に設定された有効なルールの総数が表示されることに注意してください。また、パッシブ展開では、[ドロップしてイベントを生成する（Drop and Generate Events）] に設定されたルールで行われるのはイベントの生成のみであることにも注意してください。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　ルール状態を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　ルール状態を設定する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　次の選択肢があります。

- トラフィックが選択されたルールと一致したときにイベントを生成するには、[ルール状態（Rule State）] > [イベントを生成する（Generate Events）] の順に選択します。
- インライン展開でトラフィックが選択されたルールと一致したときにイベントを生成し、そのトラフィックをドロップするには、[ルール状態（Rule State）] > [ドロップしてイベントを生成する（Drop and Generate Events）] の順に選択します。
- 選択されたルールと一致するトラフィックを検査しないようにするには、[ルール状態（Rule State）] > [無効（Disable）] の順に選択します。

（注）　シスコ 侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨します。すべてのルールが有効になっている場合は、管理対象デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

手順 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

ポリシー単位の侵入イベント通知のフィルタリング

ライセンス：Protection

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

詳細については、次の各項を参照してください。

- イベントしきい値の設定（32-26 ページ）では、発生回数に基づくイベントの表示頻度を指定するしきい値の設定方法について説明します。イベント単位およびポリシー単位でしきい値を設定できます。
- 侵入ポリシー単位の抑制の設定（32-31 ページ）では、指定されたイベントの通知を各ポリシー内の送信元 IP アドレス単位または宛先 IP アドレス単位で抑制する方法について説明します。

イベントしきい値の設定

ライセンス：Protection

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。しきい値は、共有オブジェクトのルール単位、標準テキスト ルール単位、またはプリプロセッサ ルール単位で設定できます。

詳細については、次の項を参照してください。

- イベントしきい値の設定について（32-26 ページ）
- 侵入イベントしきい値の追加と変更（32-28 ページ）
- 侵入イベントしきい値の表示と削除（32-30 ページ）
- ルールのしきい値の設定（32-7 ページ）

イベントしきい値の設定について

ライセンス：Protection

まず、しきい値タイプを指定する必要があります。次の表に示すオプションの中から選択できます。

表 32-6　しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
両方	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [両方（Both）] に、[カウント（Count）] を 2 に、[秒（Seconds）] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定する必要があります。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。次の表の中から、システムがイベント インスタンスを追跡する方法を指定するためのオプションの 1 つを選択します。

表 32-7　IP しきい値設定オプション

オプション	説明
ソース（Source）	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
[接続先（Destination）]	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 32-8　インスタンス/時間のしきい値設定オプション

オプション	説明
メンバー数（Count）	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。
秒（Seconds）	カウントがリセットされるまでの秒数。しきい値タイプを [制限（limit）] に、トラッキングを [送信元 IP（Source IP）] に、[カウント（count）] を 10 に、[秒（seconds）] を 10 に設定した場合は、システムが指定された送信元ポートから 10 秒間に発生した最初の 10 のイベントを記録して表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベント抑制のいずれかと組み合わせて使用することもできます。詳細については、動的ルール状態の追加（32-34 ページ）、イベントのフィルタリング（36-96 ページ）、および侵入ポリシー単位の抑制の設定（32-31 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入イベントしきい値の追加と変更（32-28 ページ）
- ルールのしきい値の設定（32-7 ページ）
- 侵入イベントしきい値の表示と削除（32-30 ページ）

ヒント　侵入イベントのパケット ビューでしきい値を追加することもできます。詳細については、イベント情報の表示（41-27 ページ）を参照してください。

侵入イベントしきい値の追加と変更

ライセンス：Protection

1 つ以上の特定のルールのしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに 1 つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

しきい値設定の表示方法と削除方法については、侵入イベントしきい値の表示と削除（32-30 ページ）を参照してください。

また、すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。詳細については、侵入イベント ロギングのグローバルな制限（35-1 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ヒント　複数の CPU を搭載した管理対象デバイスでグローバルしきい値または個別のしきい値を設定すると、予想より多くのイベントが生成される場合があります。

イベントしきい値を追加または変更する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [侵入(Intrusion)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

手順 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　しきい値を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて(32-11 ページ)および侵入ポリシー内のルール フィルタの設定(32-22 ページ)を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

手順 5　しきい値を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　[イベント フィルタリング(Event Filtering)] > [しきい値(Threshold)] の順に選択します。

[しきい値(thresholding)] ポップアップ ウィンドウが表示されます。

手順 7　[タイプ(Type)] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[制限(Limit)] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[しきい値(Threshold)] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[両方(Both)] を選択します。

手順 8　[追跡対象(Track By)] ドロップダウンリストから、イベント インスタンスが**送信元** IP アドレスまたは**宛先** IP アドレスのどちらによって追跡されるかを選択します。

手順 9　[カウント(Count)] フィールドで、しきい値として使用するイベント インスタンスの数を指定します。

手順 10　[秒(Seconds)] フィールドで、イベント インスタンスを追跡する期間を表す秒数を指定します。

手順 11　[OK] をクリックします。

システムが、しきい値を追加し、[イベント フィルタリング(Event Filtering)] カラムのルールの横にイベント フィルタ アイコン( )を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

手順 12　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

侵入イベントしきい値の表示と削除

ライセンス：Protection

既存のしきい値設定を表示または削除することができます。[ルールの詳細（Rules Details）] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできることに注意してください。詳細については、侵入イベント ロギングのグローバルな制限（35-1 ページ）を参照してください。

しきい値を表示または削除する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　表示または削除する、しきい値が設定されたルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　選択したルールのしきい値を削除するには、[イベント フィルタリング（Event Filtering）] > [しきい値の削除（Remove Thresholds）] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。

ヒント　特定のしきい値を削除するために、ルールを強調表示して、[詳細の表示（Show Details）] をクリックすることもできます。しきい値設定を展開して、削除するしきい値設定の横にある [削除（Delete）] をクリックします。[OK] をクリックして、設定の削除を確認します。

ページが更新され、しきい値が削除されます。

手順 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

侵入ポリシー単位の抑制の設定

ライセンス：Protection

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、特定のエクスプロイトのように見えるパケットを伝送しているメール サーバが存在する場合は、そのメール サーバによってトリガーとして使用されたイベントに関するイベント通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、`detection_filter` キーワード、および侵入イベントしきい値構成のいずれかと組み合わせて使用することもできることに注意してください。詳細については、動的ルール状態の追加（32-34 ページ）、イベントのフィルタリング（36-96 ページ）、およびイベントしきい値の設定（32-26 ページ）を参照してください。

詳細については、次の各項を参照してください。

- 侵入イベントの抑制（32-31 ページ）
- 抑制条件の表示と削除（32-33 ページ）

ヒント　侵入イベントのパケット ビューで抑制を追加することもできます。詳細については、イベント情報の表示（41-27 ページ）を参照してください。また、[ルール エディタ（Rule Editor）] ページや任意の侵入イベント ページ（イベントが侵入ルールによってトリガーされた場合）で右クリック コンテキスト メニューを使用して、抑制設定にアクセスすることもできます。

侵入イベントの抑制

ライセンス：Protection

ルールに関する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン( )が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベント表示を抑制する方法:

アクセス: Admin/Intrusion Admin

手順 1　[ポリシー(Policies)] > [侵入(Intrusion)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。

[侵入ポリシー(Intrusion Policy)] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン( )をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定(23-17 ページ)を参照してください。

[ポリシー情報(Policy Information)] ページが表示されます。

手順 3　[ルール(Rules)] をクリックします。

[ルール(Rules)] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

手順 4　抑制を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて(32-11 ページ)および侵入ポリシー内のルール フィルタの設定(32-22 ページ)を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　抑制条件を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　[イベント フィルタリング(Event Filtering)] > [抑制(Suppression)] の順に選択します。

[抑制(suppression)] ポップアップ ウィンドウが表示されます。

手順 7　次の [抑制タイプ(Suppression Type)] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[ルール(Rule)] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[送信元(Source)] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[宛先(Destination)] を選択します。

手順 8　抑制タイプとして [送信元(Source)] または [宛先(Destination)] を選択した場合は、[ネットワーク(Network)] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

FireSIGHT システムで IPv4 CIDR と IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則(1-24 ページ)を参照してください。

手順 9　[OK] をクリックします。

システムが、抑制条件を追加し、抑制するルールの横にある [イベント フィルタリング（Event Filtering）] カラムのルールの横にイベント フィルタ アイコン（）を表示します。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

手順 10　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

抑制条件の表示と削除

ライセンス：Protection

既存の抑制条件を表示または削除することもできます。たとえば、メール サーバがエクスプロイトのように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメール サーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

定義された抑制条件を表示または削除する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。デフォルトで、ページにはルールがメッセージのアルファベット順に一覧表示されます。

手順 4　抑制を表示または削除するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　抑制を表示または削除する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　次の 2 つの対処法があります。

- ルールのすべての抑制を削除するには、[イベント フィルタリング（Event Filtering）] > [抑制の削除（Remove Suppressions）] を選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。
- 特定の抑制設定を削除するには、ルールを強調表示して、[詳細の表示（Show Details）] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [削除（Delete）] をクリックします。[OK] をクリックして、選択した設定の削除を確認します。

ページが更新され、抑制設定が削除されます。

手順 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

動的ルール状態の追加

ライセンス：Protection

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レート ベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

詳細については、次の項を参照してください。

- 動的ルール状態について（32-34 ページ）
- 動的ルール状態の設定（32-36 ページ）

動的ルール状態について

ライセンス：Protection

侵入ポリシーにレート ベースのフィルタを含めることにより、一定期間においてルールの一致が過剰に発生した時点を検出できます。インライン展開された管理対象デバイスでこの機能を使用すると、指定した時間だけレートベース攻撃をブロックし、その後、ルールが一致した場合にイベントの生成のみを行う、トラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（[イベントを生成する（Generate Events）]、[ドロップしてイベントを生成する（Drop and Generate Events）]、および [無効（Disable）] の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達すると、レートがしきい値を下回っていれば、ルールのアクションがルールの初期設定に戻ります。

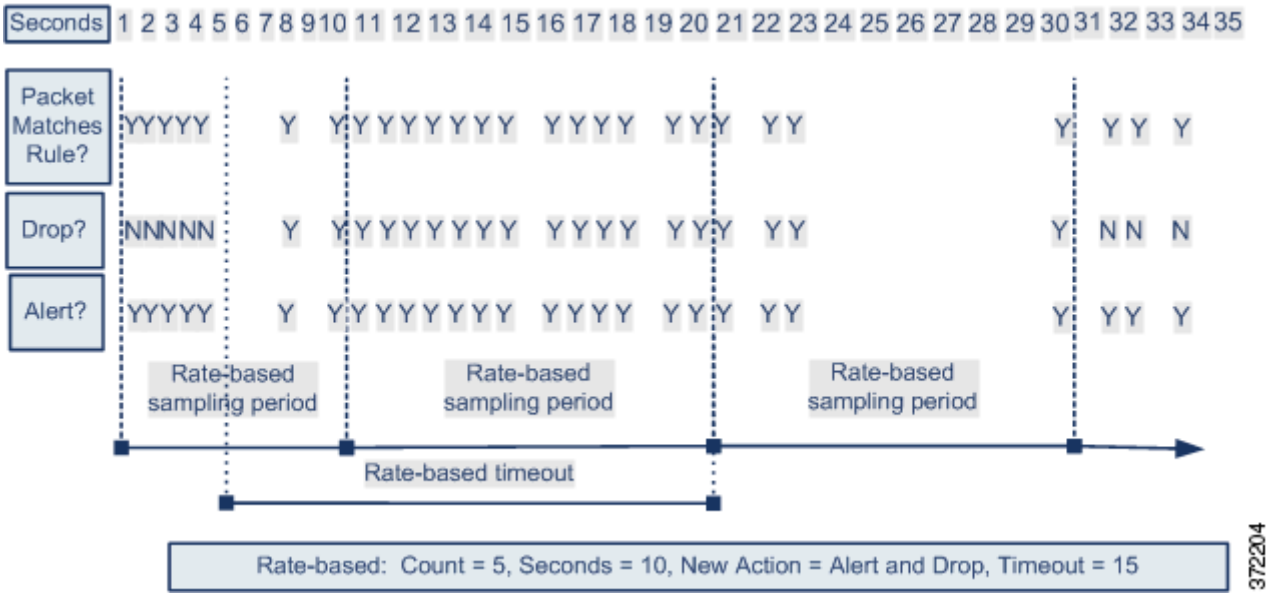
インライン展開のレート ベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[イベントを生成する（Generate Events）] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしません。ただし、攻撃トラフィックが、レート ベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

(注)　レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレート ベースのフィルタを定義できます。侵入ポリシーに列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。パスワードを検出しようとする試行が繰り返されると、レート ベース攻撃防止が設定されたルールがトリガーされます。レート ベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [ドロップしてイベントを生成する（Drop and Generate Events）] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレート ベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[イベントを生成する（Generate Events）] に戻ります。



動的ルール状態の設定

ライセンス：Protection

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを [ドロップしてイベントを生成する（Drop and Generate Events）] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

アクションの変更をトリガーするために特定のヒット数が発生する必要のあるカウントと秒数を指定することによって、そのルールのヒット数を設定します。加えて、タイムアウトが発生したらアクションをルールの以前の状態に戻すタイムアウトを設定できます。

同じルールに対して複数の動的状態フィルタを定義できます。侵入ポリシー内のルール詳細に列挙された最初のフィルタに最も高い優先度が割り当てられます。2 つのレート ベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（ ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

動的ルール状態を追加する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。

手順 4　動的ルール状態を追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　動的ルール状態を追加する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　[動的状態（Dynamic State）] > [レート ベースのルール状態の追加（Add Rate-Based Rule State）] の順に選択します。

[レート ベースのルール状態の追加（Add Rate-Based Rule State）] ダイアログボックスが表示されます。

手順 7　[追跡対象（Track By）] ドロップダウンリストから、ルール一致の追跡方法を選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[送信元（Source）] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[宛先（Destination）] を選択します。
- そのルールのすべての一致を追跡する場合は、[ルール（Rule）] を選択します。

手順 8　[追跡対象（Track By）] を [送信元（Source）] または [宛先（Destination）] に設定した場合は、[ネットワーク（Network）] フィールドに追跡する各ホストのアドレスを入力します。

単一の IP アドレス、アドレス ブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。FireSIGHT システムで IPv4 CIDR と IPv6 プレフィックス長アドレス ブロックを使用する方法については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 9　[レート（Rate）] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [カウント（Count）] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [秒（Seconds）] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

手順 10　[新しい状態（New State）] ドロップダウンリストから、条件が満たされたときに実行すべき新しいアクションを指定します。

- イベントを生成する場合は、[イベントを生成する（Generate Events）] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットをドロップする場合、または、パッシブ展開でイベントを生成する場合は、[ドロップしてイベントを生成する（Drop and Generate Events）] を選択します。
- アクションを実行しない場合は、[無効（Disabled）] を選択します。

手順 11　[タイムアウト（Timeout）] フィールドに、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[タイムアウト（Timeout）] フィールドを空白のままにします。

手順 12　[OK] をクリックします。

システムが、動的ルール状態を追加し、[動的状態（Dynamic State）] カラムのルールの横に動的状態アイコン（）を表示します。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラー メッセージが表示されます。

ヒント　一連のルールのすべての動的ルール設定を削除するには、[ルール（Rules）] ページでルールを選択してから、[動的状態（Dynamic State）] > [レート ベース状態の削除（Remove Rate-Based States）] の順に選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[詳細の表示（Show Details）] をクリックしてから、削除するレート ベースのフィルタのそばにある [削除（Delete）] をクリックします。

手順 13　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

SNMP アラートの追加

ライセンス：Protection

FireSIGHT システム に対して SNMP アラートを設定する場合は、ルールによってイベントが生成されたときに SNMP アラートを発生する特定のルールを設定できます。詳細については、SNMP 応答の使用（44-2 ページ）を参照してください。

SNMP アラートを設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。

手順 4　SNMP アラートを設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　SNMP アラートを設定する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　[アラート（Alerting）] > [SNMP アラートの追加（Add SNMP Alert）] の順に選択します。

システムが、アラートを追加し、[アラート（Alerting）] カラムのルールの横にアラート アイコン（）を表示します。ルールに複数のアラート タイプを追加した場合は、アイコン上の数字がアラート タイプの数を示します。

ヒント　ルールから SNMP アラートを削除するには、そのルールの横にあるチェックボックスをクリックして、[アラート（Alerting）] > [SNMP アラートの削除（Remove SNMP Alerts）] の順に選択してから、[OK] をクリックして削除を確認します。

手順 7　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。

ルール コメントの追加

ライセンス：Protection

ルールにコメントを追加することができます。追加したコメントは、[ルール（Rules）] ページ上の [ルールの詳細（Rule Details）] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [編集（Edit）] ページで [ルール コメント（Rule Comment）] をクリックしてコメントを表示することもできます。ルールの編集の詳細については、既存のルールの変更（36-114 ページ）を参照してください。

コメントをルールに追加するには、次の手順を実行します。

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　[ルール（Rules）] をクリックします。

[ルール（Rules）] ページが表示されます。

手順 4　コメントを追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタリングについて（32-11 ページ）および侵入ポリシー内のルール フィルタの設定（32-22 ページ）を参照してください。

  ページが更新され、一致するすべてのルールが表示されます。

手順 5　コメントを追加する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェックボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェックボックスをオンにします。

手順 6　[コメント（Comments）] > [ルール コメントの追加（Add Rule Comment）] の順に選択します。

[コメントの追加（Add Comment）] ダイアログボックスが表示されます。

手順 7　[コメント（Comments）] フィールドに、ルール コメントを入力します。

手順 8　[OK] をクリックします。

システムが、コメントを追加し、[コメント（Comments）] カラムのルールの横にコメント アイコン（ ）を表示します。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント　ルール コメントを削除するには、そのルールを強調表示して、[詳細の表示（Show Details）] をクリックしてから、[コメント（Comments）] セクションで [削除（Delete）] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

手順 9　ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理（31-3 ページ）」と「侵入ポリシーの編集（31-4 ページ）」を参照してください。